UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,667	02/05/2004	Mukesh Kumar Singh	TI-35979	5588

23494 7590 07/30/2008

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	**PAPER NUMBER**
2135	

NOTIFICATION DATE	DELIVERY MODE
07/30/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com
uspto@dlemail.itg.ti.com

Office Action Summary	Application No.	Applicant(s)	
	10/772,667	SINGH, MUKESH KUMAR	
	Examiner	Art Unit	
	SUMAN DEBNATH	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 are pending in this application.

2. Claims 1 and 13 are currently amended.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/01/2008 has been entered.

Claim Objections

4. Claims 3-4 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative only. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-8 and 13-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Brandstrom (Patent No.: 4,322,577).

7. As to claim 1, Brandstrom discloses a method of encryption (abstract), comprising:

(a) partitioning an input message into matrix elements (col. 3, lines 40-45);

(b) computing a determinant of said matrix (col. 6, lines 4-10 and lines 55-63);

(c) encrypting said determinant (col. 7, lines 16-30); and

(d) multiplying said matrix by said encrypted determinant (col. 6, lines 40-45 and col. 7, lines 16-30).

8. As to claim 2, Brandstrom discloses further comprising, preprocessing said input message wherein said preprocessing includes a permutation of the message (col. 7, lines 4-15).

9. As to claim 3, Brandstrom discloses wherein: (a) said permutation of step (a) of claim 2 is generated by a hash of said input message (col. 6, lines 40-45 and col. 7, lines 16-30).

10. As to claim 4, Brandstrom discloses wherein: (a) said permutation of step (a) of claim 2 is generated by a random sequence (col. 6, lines 55-63).

11. As to claim 5, Brandstrom discloses wherein: (a) said preprocessing of step (a) of claim 2 includes exclusive ORing said message after permutation with generators of said permutation (col. 7, lines 29-65).

12. As to claim 6, Brandstrom discloses wherein: (a) said encrypting of step (c) of claim 1 is public-key encryption (col. 7, lines 29-65).

13. As to claim 7, Brandstrom discloses wherein: (a) said public-key encryption is RSA (col. 7, lines 29-65).

14. As to claim 8, Brandstrom discloses wherein: (a) said partitioning of step (a) of claim 1 first fills the principal diagonal of said matrix (col. 7, lines 29-65).

15. As to claim 13, Brandstrom discloses a method of decrypting, comprising:

(a) computing a determinant of a matrix-based encrypted message matrix, wherein said encrypted message was .generated by partitioning an input message into matrix elements (col. 7, lines 29-38);

(b) decrypting said determinant (col. 6, lines 40-45 and col. 7, lines 16-30); and

(c) multiplying said matrix by the results of step (b) (col. 6, lines 40-45 and col. 7, lines 16-30).

16. As to claim 14, Brandstrom discloses wherein: (a) when said matrix-based encrypted message of step (a) of claim 13 had preprocessing including a permutation, applying the inverse of said permutation to the results of step (c) of claim 13 (col. 6, lines 40-45 and col. 7, lines 16-30).

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 9-12 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boylan et al. (Pub. No.: US 2003/0028484 A1) (hereinafter "Boylan") and further in view of Chung (Pub. No.: US 2003/0016823 A1).

19. As to claim 9, Boylan discloses a method of encryption, comprising:

(a) defining a permutation source ([0008], lines 14-15);

(b) generating a permuted message for an input message employing said permutation source ([0008], lines 14-15);

(c) padding said permuted message with said permutation source to obtain a preprocessed message ([0008], lines 16-18).

Although Boylan discloses encrypting said preprocessed message ([0008], lines 20-21), Boylan doesn't explicitly disclose (d) encrypting said preprocessed message

with block-based encryption method which has blocks smaller than said preprocessed message.

However, Chung discloses (d) encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message ([0011], Chung provides DES as block-based encryption which divides long message into smaller blocks and encrypts the individual blocks).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Boylan as taught by Chung in order to encrypt long messages by taking advantage of standard block-based encryption method.

20. As to claim 10, Boylan discloses wherein: said permutation source is generated by a hash of said input message ([0008], lines 14-15).

21. As to claim 11, Boylan discloses wherein: said permutation source is generated by a random sequence ([0008], lines 14-15).

22. As to claim 12, Boylan discloses wherein: said block-based encryption is a public key encryption ([0008]).

23. As to claim 15, Boylan discloses wherein said padding includes prepending said permuted message with said permutation source to obtain said preprocessed message ([0008], lines 14-15).

24. As to claim 16, Boylan discloses wherein said padding includes appending said permuted message with said permutation source to obtain said preprocessed message ([0008]).

Response to Arguments

25. Applicant's arguments with respect to claims 1-16 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2135

/H. S./

Primary Examiner, Art Unit 2135